

**DETAILED ACTION**

***Claim Objections***

1. Claims 12 and 18 are objected to because of the following informalities: Applicant is requested to clearly identifying the claimed invention. For example, applicant is claiming a storing unit, and an internal communication unit in claims 12 and 18, respectively. It is unclear if applicant is referring to item 1122 or 1011 for the storing unit, and 1113 or 1013 for the communication unit. For the purpose of examination, it was assumed that applicant is referring to item 1122 for the storing unit and 1113 for the communication unit. Appropriate correction is required.

***Claim Rejections - 35 USC § 102***

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102a that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

3. Claims 1, 4, 5, 6, 14, 16, 18 -21, 23, 25, 27 29-32, are rejected under 35 U.S.C. 102(a) as being anticipated by Tamada in EP 393660.

Consider Claims 1, 4, 16, 18, and 23, Tamada discloses an authenticating system, comprising, an electric license card (10) providing a storing unit (15a and 15b) included in an electric license card of storing license card information and security code

for reading out said license card information, (See Tamada, abstract, col. 2 I 49 – col. 3 I. 18, where Tamada discusses an electronic driver's license comprising a memory for storing license information and security code for reading out license information). Tamada discloses a communicating unit included in the electric license card of communicating with a vehicle or in-vehicle apparatuses, (See Tamada, col. 2 I 49 – col. 3 I. 18, where Tamada discusses a readout unit in the electric license IC card of communicating with a readout unit 22 of restriction apparatus 20). Tamada discloses a security code authenticating unit for controlling transmitting by said communicating unit included in said electric license card, (See Tamada, col. 2 I 49 – col. 3 I. 18, col. 4 I. 20 – 30, where Tamada discusses a control unit 14 in the electric license IC card of for authenticating a security code). Tamada discloses an authenticating device providing a communicating unit mounted in the authenticating device, (See Tamada, col. 2 I 40 – 48, where Tamada discusses a restriction apparatus 20 comprising a readout unit 22). Tamada discloses a security code inputting unit of inputting security code, (See Tamada, col. 2 I 40 – 48, where Tamada discusses the restriction apparatus 20 comprising a keyboard 23). Tamada discloses a storing unit mounted on said authenticating device of storing said security code inputted from said security code inputting unit a security code, (See Tamada, col. 2 I 40 – 48, col. 3 I. 48, where Tamada discusses the restriction apparatus 20 comprising a memory 24 for storing security code inputted from keyboard). Tamada discloses transmitting unit of transmitting said security code stored in said storing unit mounted on said authenticating device to said communicating unit mounted

on said authenticating device, (**See Tamada, col. 2 I 40 – 48, col. 3 I. 48, col. 4 I. 15-30, where Tamada discusses the restriction apparatus 20 comprising a control unit 21 for transmitting information from keyboard 23 to readout section 22 of the restriction apparatus**). Tamada discloses a person authenticating unit of authenticating said license card information, and of activating the in-vehicle apparatuses, characterized by said storing unit included in said electric license card being operative to store function information informing about function of the vehicle, (**See Tamada, col. 2 I 40 – 48, col. 3 I. 48, col. 4 I. 15-53, where Tamada discusses the control unit 21 for authenticating license information, and activating the vehicle as describe by information stored in memory 15**). Tamada discloses said communicating unit mounted on said authenticating device being operative to transmit said security code transmitted from said security code transmitting unit to said electric license card, (**See Tamada, col. 2 I 40 – 48, col. 3 I. 48, col. 4 I. 15-30, where Tamada discusses the restriction apparatus 20 comprising a control unit 21 for transmitting information from keyboard 23 to readout section 22 to the electronic driver's license 10**). Tamada discloses said security code authenticating unit is operative to determine whether or not said security code transmitted from said authenticating device agrees with security code stored in said storing unit included in said electric license card, (**See Tamada, col. 2 I 49 – col. 3 I. 18, col. 4 I. 20 – 30, where Tamada discusses the control unit 14 determine whether or not security code transmitted from the restriction apparatus agrees with security code stored in the memory unit 15 of electric license card**). Tamada discloses transmits said

license card information and the function information when said security code authenticating unit determines said security code transmitted from said authenticating device agrees with security code stored in said storing unit included in said electric license card, (See Tamada, abstract, col. 2 l 49 – col. 3 l. 18, col. 4 l. 20 – col. 5 l. 53, where Tamada discusses a transmission of license card and vehicle authorization information when the control unit 14 determines the security code transmitted from the restriction apparatus agrees with security code stored in the memory unit 15 of electric license card). Tamada discloses said communicating unit mounted on said authenticating device is operative to receive said license card information and said activating information informing said function to be activated, (See Tamada, col. 2 l 40 – 48, col. 3 l. 48, col. 4 l. 15-30, where Tamada discusses the readout section 22 receives license card and authorization information and for activating the locks and engine). Tamada discloses said person authenticating unit is operative to activate said in-vehicle apparatuses designated by said function information when said person authenticating unit correctly authenticates said license card information, (See Tamada, col. 2 l 40 – 48, col. 3 l. 48, col. 4 l. 15-53, where Tamada discusses the control unit 21 activates the locks and engine based on the license card information).

Consider claims 27 and 29, Tamada discloses an authenticating method of authenticating license card information by communicating between an electric license card storing license card information including driver identifying information, and said

vehicle or said in-vehicle apparatuses mounted on said vehicle, (**See Tamada, abstract, col. 2 I 49 – col. 3 I. 18, where Tamada discusses a method of authenticating electronic license card 10 by communicating between the license card storing driver's information and a restriction apparatuses 20 of the vehicle**). Tamada discloses in-vehicle apparatuses mounted on said vehicle comprising an authenticating step of authenticating said license card information in said vehicle or said in-vehicle apparatuses, (**See Tamada, col. 2 I 49 – col. 3 I. 18, col4 I. 12-30, where Tamada discusses a step of authenticating electronic license card information in the restriction apparatuses 20 of the vehicle**). Tamada discloses an informing step of informing said license card information and said function information to said vehicle or said in-vehicle apparatuses mounted on said vehicle when said electric license card determines that said security code transmitted from said vehicle or said in-vehicle apparatuses mounted on said vehicle agrees with said security code stored in said electric license card, (**See Tamada, col. 4 I. 12-30, where Tamada discusses a step of informing the card information and operation permission to the restriction apparatus when the license card determines that the code number transmitted from restriction apparatus agrees with the code number stored in the license card**). Tamada discloses a receiving step of receiving said license card information and function information designating said in-vehicle apparatuses to be activated by said vehicle or said in-vehicle apparatuses mounted on said vehicle, (**See Tamada, col. 4 I. 12-30, where Tamada discusses a step of receiving the card information and operation permission allowing the restriction apparatus to be activate**). Tamada

discloses an activating step of activating said in-vehicle apparatuses designated by function information when said vehicle or said in-vehicle apparatuses correctly authenticates said license card information, (**See Tamada, col. 4 l. 12-30, where Tamada discusses a step of activating the key lock section 25 and engine control section 26 when the restriction apparatus authenticates electronic license information).**

Consider claims 5, and 30-32, Tamada discloses the authenticating apparatus as set forth in claim 1, in which said activating unit is connected to an engine control apparatus for controlling an engine of said vehicle, and is operative to activate said engine, when said authenticating unit correctly authenticates said license card information, (**See Tamada, col. 2 l. 40 – 48, col. 3 l. 48, col. 4 l. 15-53, where Tamada discusses the control unit 21 activates the engine based on the license card information once the control unit authenticate the information).**

Consider claim 14, and 25, Tamada discloses the authenticating system as set forth in claim 23, which further comprises using record acquisition unit of acquiring using record of said in-vehicle apparatuses activated by said electric license card according to the user, and said security code transmitting unit is operative to transmit security code in dating order of using record stored in said storing unit mounted on said authenticating device, (**See Tamada, col. 3 l. 22 – 48, where Tamada discusses the control unit 21**

**is operable to keep record of transaction and store authenticating result such as the History information EHI and HI of the electronic license 10).**

Consider claim 19, Tamada discloses the authenticating system as set forth in claim 18, in which said authenticating unit [1123] is operative to transmit authenticating result as reserving of using said in-vehicle apparatuses to said electric license card, (See Tamada, col. 3 l. 22 – 48, col. 6 l. 45-54, where Tamada discusses the control unit 21 is operable to transmit and store authenticating result such as the History information EHI and HI of the electronic license 10).

Consider claim 20, Tamada discloses the authenticating system as set forth in claim 18, in which said authenticating device [1123] is operative to transmit operating information [transmit to what?] informing whether or not said in-vehicle apparatuses have been activated as a result of authenticating, (See Tamada, col. 6 l. 34-54, col. 7 l. 31 – 35, where Tamada discusses the control unit 21 is operable to transmit the authenticating result informing the driver whether or not the access is granted).

Consider claim 21, Tamada discloses the authenticating system as set forth in one of claims 18-20, in which said authenticating device [1123] is operative to store activating information informing which of in-vehicle apparatuses can be activated according to said electric license card, and controls activating of said in-vehicle apparatuses according to said electric license card, (See Tamada, col. 3 l. 22 – 48, col.

**6 I. 45-54, where Tamada discusses the control unit 21 is operable to transmit and store authenticating result such as the History information EHI and HI of the electronic license 10).**

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 12, are rejected under 35 U.S.C. 103(a) as being unpatentable over Tamada in EP 393660.

With respect to the limitations in claim 12; Tamada discloses an information registering/deleting means [in-vehicle per spec item 3034] for registering said security code and said personal information read out from said electric license card in response to said security code inputted from said security code inputting means in said storing unit [claim 12, which storing unit ? for the purpose of examination storing unit mounted in-vehicle apparatus], (See Tamada, col. 2 I 40 – 48, col. 3 I. 48, col. 4 I. 15-53, col. 5 I. 8-18, where Tamada discusses the restriction apparatus 20 is capable to register and compare the security code and said personal information that reads out from said electric license card in response to the security code inputted from

**keyboard in the storing unit of restriction apparatus 20 and the owner of the vehicle can grant the use of the vehicle to other person).** The examiner takes official notice that the owner of the vehicle should be able to restrict the use of the vehicle. Tamada does not explicitly discloses deleting said security code and said personal information registered in said storing unit [mounted in-vehicle apparatus], however it would be obvious if the owner of the vehicle can grant the use of the vehicle to other users then the owner should be able to restrict the use of the vehicle; therefore, deleting security code information that are registered for other users. (**See col. 4. l. 49-50).**

6. Claims 2, 3, 13, 17, 24, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tamada in EP 393660, and further in view of Odaka in US 6538559.

Consider claim 2, and 17, Odaka in view of Tamada discloses the authenticating apparatus as set forth in claim 1, in which said in-vehicle communication unit is operative to transmit position information [transmit where? For the purpose of examination transmitted to the license card, per ¶ 101.] specified by a position on the outer surface of said vehicle when acquiring said license card information and said activating information, and said activating unit is operative to activate functions designated by said activating information transmitted from said electric license card in accordance with said position information, (**See Odaka, abstract, Fig 4 & 5, col. 5 l. 15-55, where Odaka discusses a first request signal is transmitted when the**

**mobile unit is outside vehicle the system identifies the location of mobile unit with respect to the vehicle and acquiring first code for unlocking the doors).**

Consider claims 2, 3, 6, 13, 17, 24, and 28, it would be obvious to one of ordinary skilled artisan at the time of invention to modify Tamada and a first request signal from outside for unlocking the door, and a second request signal transmitted when the mobile unit is inside vehicle for unlocking the steering wheel and where the mobile unit storing the code communicates with the vehicle transmitter in RF frequency as taught by Odaka, (**See Odaka, col. 1. l. 42-50, col. 2 l. 8-21, where he discusses the reason for his invention for designing a RF communication system where a diagnosing system can easily determine a failure of transmission between a transponder and a reader; therefore, designing a user friendly system for user convenience. Odaka and Tamada are from the same field endeavor because both of them are teaching a system and method of accessing a vehicle).**

Consider claim 3, Odaka in view of Tamada the authenticating apparatus as set forth in claim 2, in which said in-vehicle communicating unit is operative to transmit said position information [to the electric license card], when said electric license card is existing adjacent to said in-vehicle communicating unit, and said authenticating unit is operative to authenticate said license card information, when request for authenticating is issued from said electric license card, (**See Odaka, abstract, Fig 4 & 5, col. 5 l. 56 – col. 6 l. 12, where Odaka discusses a second request signal transmitted when the**

**mobile unit is inside vehicle the system identifies the vicinity of mobile unit with respect to the instrument panel of the vehicle and acquiring second code for unlocking the steering wheel).**

Consider claim 6, Tamada discloses the authenticating apparatus as set forth in one of claims 1-5, in which said activating unit is connected to a door and is operative to authenticating unit correctly authenticates said license card information, (**See Tamada, col. 2 l. 49-52, col. 3 l. 49-53, where Tamada discusses the readout section 22 is located outer surface of the door and the control unit 21 activates the key lock section 25 that unlocks the steering wheel based on the license card information once the control unit authenticates the information**). Tamada does not explicitly discloses that the key lock section 25 is used to unlock the doors; however, Odaka discloses unlocking apparatus for unlocking doors of said vehicle, and is operative to unlock said doors, when said authenticating unit correctly authenticates said license card information, (**See Odaka, abstract, Fig 4 & 5, col. 5 l. 15-55, where Odaka discusses a request signal is transmitted when the mobile unit is outside vehicle the system identifies the location of mobile unit with respect to the vehicle and acquiring first code for unlocking the doors**).

Consider claim 13, and 24, Odaka in view of Tamada discloses the authenticating apparatus as set forth in claim 23, which further comprises a using frequency acquisition means of acquiring using frequency of said in-vehicle apparatuses

activated by said electric license card according to the user, and said security code transmitting unit being operative to transmit security code in decreasing order by using frequency stored in said storing unit mounted on said authenticating device, (See **Odaka, abstract, Fig 4 & 5, col. 5 I. 15-55, where Odaka discusses the receiving antenna of the mobile unit 60 receives a request signal with a frequency of 134 kHz, which has been modulated from the first request code by the vehicle transmitter).**

Consider claim 28, Odaka in view of Tamada discloses the authenticating method as set forth in claim 27, which further comprises a position informing step of informing position information showing position of said electric license card to said vehicle or said in-vehicle apparatuses mounted on said vehicle, and said electric license card informs function corresponding to said position information to said vehicle or said in-vehicle apparatuses mounted on said vehicle, (See **Odaka, abstract, Fig 4 & 5, col. 5 I. 15-55, where Odaka discusses a step where a first request signal is transmitted when the mobile unit is outside vehicle the system identifies the location of mobile unit with respect to the vehicle's outside parameter and acquiring first code for unlocking the doors).**

7. Claims 7, are rejected under 35 U.S.C. 103(a) as being unpatentable over Tamada in EP 393660, further in view of Odaka in US 6538559, and further in view of Cambier et al. in US 6532298.

Consider claim 7, Cambier in view of Tamada and Odaka discloses the authenticating apparatus as set forth in one of claims 1-5, in which said activating unit is connected to an in-vehicle telephone apparatus, and is operative to activate said in-vehicle telephone apparatus, when said authenticating unit correctly authenticates said license card information, however, Yamagishi teaches these limitations, (**See Cambier , where discusses a portable authentication device used to access a cellular telephone, a vehicle, or other asset where it is used to authenticate user and eliminate theft**).

It would be obvious to one of ordinary skilled artisan at the time of invention to modify Tamada and allow the hand held device to access a cellular telephone and a vehicle as taught by Cambier, (**See col. 1 41-64, where he discusses the reason for his invention for designing a portable authentication device to access multiple assets with bio metric security features; therefore, providing safety and convenience to the user. Cambier and Tamada are from the same field endeavor because both of them are teaching a system and method of accessing a vehicle**).

8. Claims 8-11, are rejected under 35 U.S.C. 103(a) as being unpatentable over Tamada in EP 393660, further in view of Odaka in US 6538559, and further in view of Yamagishi in US 7142089.

Consider claim 8, Yamagishi in view of Tamada and Odaka discloses the authenticating apparatus as set forth in one of claims 1-5, in which said activating unit is connected to an in-vehicle audio apparatus, and is operative to activate said in-vehicle audio apparatus, when said authenticating unit correctly authenticates said license card information, (**See Yamagishi, abstract, col. 5 l. 26-47, where Yamagishi discusses controller 7 is connected to a vehicle's mobile communication terminal 35 is configured for a mobile telephone comprising an audio feature that is activated by controller upon proper access of the vehicle**).

Consider claims 8-11, it would be obvious to one of ordinary skilled artisan at the time of invention to modify Tamada and include a controller that is connected to a vehicle's mobile communication terminal configured to download authentication information, a vehicle speed sensor, and a vehicle's collision sensors 25 as taught by Yamagishi, (**See Yamagishi, col. 1 l. 45-49, where he discusses the reason for his invention for designing a vehicle communication system where a user can access enable operations of the vehicle far away from the vehicle and determine the status of the vehicle; therefore, providing convenience to the user. Yamagishi and Tamada are from the same field endeavor because both of them are teaching a system and method of accessing a vehicle**).

Consider claim 9, Yamagishi in view of Tamada and Odaka discloses the authenticating apparatus as set forth in one of claims 1-5, in which said activating unit is

connected to a combination meter apparatus, and is operative to activate said combination meter apparatus, when said authenticating unit correctly authenticates said license card information, (**See Yamagishi, abstract, col. 5 l. 16-24, where Yamagishi discusses controller 7 is connected to a vehicle speed sensor 23 that is activated by controller upon proper authentication**).

Consider claim 10, Yamagishi in view of Tamada and Odaka discloses the authenticating apparatus as set forth in one of claims 1-5, in which said activating unit is connected to an emergency report apparatus, and is operative to activate said emergency report apparatus, when said authenticating unit correctly authenticates said license card information, (**See Yamagishi, abstract, col. 5 l. 15-47, where Yamagishi discusses controller 7 is connected to a vehicle's collision sensors 25 and mobile communication terminal 35 that is configured to communication with a mobile communication network that is activated by controller upon proper access of the vehicle**).

Consider claim 11, Yamagishi in view of Tamada and Odaka discloses the authenticating apparatus as set forth in one of claims 1-5, in which said activating unit is connected to a road-vehicle communication apparatus, and is operative to activate said road-vehicle communication apparatus, when said authenticating unit correctly authenticates said license card information, (**See Yamagishi, abstract, col. 5 l. 63-67, where Yamagishi discusses controller 7 is connected to a vehicle's mobile**

**communication terminal 35 is configured for downloading authentication information from a separate database).**

9. Claim 15, is rejected under 35 U.S.C. 103(a) as being unpatentable over Tamada in EP 393660, further in view of Odaka in US 6538559 and further in view of Jakobson in US 6501380.

Consider claim 15, Jakobson in view of Tamada are Odaka discloses the authenticating apparatus as set forth in one of claims 12-14, further comprises an annunciating means for annunciating a piece of annunciation annunciating restricting of security code inputting before prohibiting of security code inputting when the number of transmitting security code from said communicating unit mounted on the in-vehicle apparatus activating device to said communicating unit on the electrical license card is exceeds a predetermined number and restricting information is issued from said electric license card to said communicating unit of said in-vehicle apparatus activating device, **(See Jakobson, col. 2 l. 5 where Jakobson discusses a warning message that indicate that the code must be entered within a certain amount of time in order to avoid stopping the operation controlling mechanism 18).**

It would be obvious to one of ordinary skilled artisan at the time of invention to modify Tamada where the code must be entered within a certain amount of time as taught by Jakobson, **(See Jakobson, col. 1 l. 20-49, where he discusses the reason for his invention for designing a system where the user is request to enter a code in order to operate the unit; therefore, providing security to the user. Jakobson**

**and Tamada are from the same field endeavor because both of them are teaching a system and method of securely gaining access of a unit).**

10. Claims 22, 26, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tamada in EP 393660, further in view of Odaka in US 6538559 and further in view of Murakami in US 6501380.

Consider claim 22, and 33, Murakami in view of Tamada discloses the authenticating system as set forth in one of claims 18-20, in which said electric license card is of a non-contact IC card type, (**See Murakami, Fig 3, Col. 11 I. 44 – col. 12 I. 31, where Murakami discusses a card key 21, can be a smart card, i.e. non-contact IC card).**

Consider claims 22, 26, and 33 it would be obvious to one of ordinary skilled artisan at the time of invention to modify Tamada where the card key can be a smart card and include a PIN rejecting unit for PIN when the PIN exceeds a predetermined number of retries, and a display unit for displaying the user entry as taught by Murakami, (**See Murakami, col. 2 I. 6-16, where he discusses the reason for his invention for designing a system that allows multiple users to gain access of a vehicle while providing adequate security and convenience to the user. Murakami and Tamada are from the same field endeavor because both of them are teaching a system and method of accessing a vehicle).**

Consider claim 26, Murakami in view of Tamada and Odaka discloses the authenticating system as set forth in one of claims 23-25, which further comprises a security code rejecting unit for rejecting further security codes when said number of continuously transmitting of security codes from said communicating unit mounted on said authenticating device to said communicating unit included in said electric license card exceeds a predetermined number, and an annunciating unit for annunciating a piece of annunciation annunciating for restricting inputting of security code before prohibiting inputting of security code, (**See Murakami, Fig 3, Col. 11 I. 44 – col. 12 I. 31, where Murakami discusses a PIN rejecting unit for rejecting further PIN when number of continuously transmitting of the PIN exceeds a predetermined number, and a display unit for displaying the user entry and error message for canceling the users request).**

#### ***Conclusion***

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US 5124920 by Tamada, Masuo et al that is a US equivalent of EP 393660.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Omer S. Khan whose telephone number is (571)270-5146. The examiner can normally be reached on M-F 7:30 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Brian A. Zimmerman can be reached on 571-272-3059. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Omer S Khan/  
Examiner, Art Unit 2612

/Brian A Zimmerman/  
Supervisory Patent Examiner, Art Unit 2612